PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04L 9/32, H04Q 7/22

A1

(11) International Publication Number: WO 99/49616

(43) International Publication Date: 30 September 1999 (30.09.99)

(21) International Application Number: PCT/US99/06426

(22) International Filing Date: 24 March 1999 (24.03.99)

(30) Priority Data:
09/047,040 24 March 1998 (24.03.98) US

(71) Applicant: ALCATEL USA SOURCING, L.P. [US/US]; 1000 Coit Road, Plano, TX 75075-5813 (US).

(72) Inventor: MILLS, Kevin, M.; 13401 Metric Boulevard, Austin, TX 78727 (US).

(74) Agents: HANLEY, Walter, J., Jr. et al.; Kenyon & Kenyon, One Broadway, New York, NY 10004 (US).

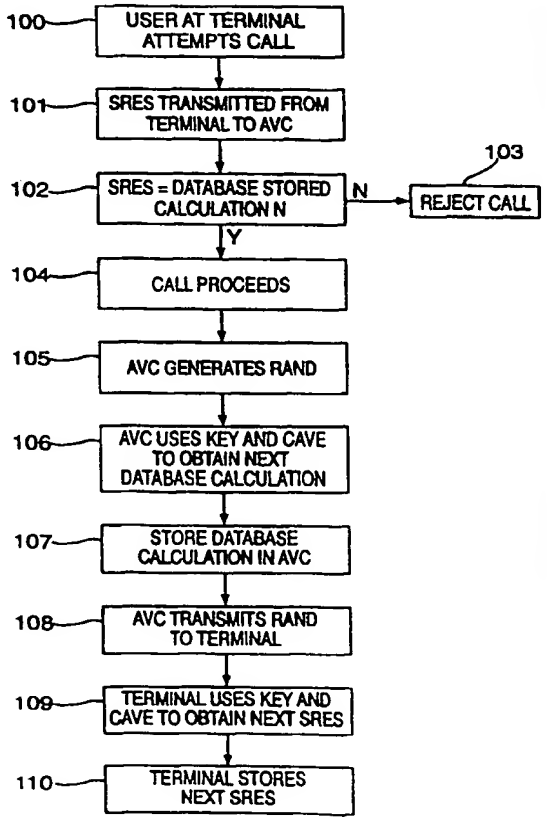
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: METHOD FOR IMPROVED AUTHENTICATION FOR CELLULAR PHONE TRANSMISSIONS

(57) Abstract

An authentication process for a cellular phone network wherein if a subscriber attempts a call (100) an encrypted result, or a signed response, previously stored in the subscriber's cell phone, is transmitted (101) to a Mobile Switching Center (MSC). If the signed response matches the encrypted result (102) previously stored in an Authentication Center (AuC) access is granted and the call proceeds (104), if not the call is rejected (103). The Authentication Center (AuC) generates a random number (105) and derives a new encrypted result by means of a CAVE algorithm using the random number and the subscriber's unique key previously stored in a database at the AuC (106). This new encrypted result is stored (107) at the AuC replacing the previously-stored encrypted result, and a Mobile Switching Center (MSC) transmits the new random number to the cellular phone (108). The cellular phone then derives a new encrypted result, or a signed response (109). The new signed result is stored in the cellular phone replacing the previously stored signed response (110).



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

METHOD FOR IMPROVED AUTHENTICATION FOR CELLULAR PHONE TRANSMISSIONS

FIELD OF THE INVENTION

The present invention relates generally to a method for providing a cellular-phone with expedited call processing and a more secure calling environment, and the present invention relates more specifically to a method for performing the transmission and calculation of messages/data utilized in an authentication procedure over more than one call so that each call proceeds faster and the decoding of the user's unique key through the scanning of any single call is made substantially impossible.

BACKGROUND INFORMATION

In recent years, the use of cellular phones for both personal and business related communication has become more popular. The obvious appeal of wireless service is the portability of the telephone, with users no longer confined to a particular space or address. However, this portability also poses a dilemma for the cellular telephone system provider, which must determine the identity of the individual making or authorizing the call for billing purposes and decide if the individual is a subscriber i.e., determine whether the individual is entitled to make the call at all.

One common way to "authenticate" callers, i.e., verify that they are who they claim to be, is set forth in FIG. 3. Each subscriber is provided with a unique, secret "key," which is also maintained in a database record kept by the cellular service provider, i.e., at the cellular service provider station. When a user wishes to make a call from a cellular terminal, i.e., when the user's phone goes off the hook, then in Step 202, the cellular-service provider transmits a signal representing a random number to the terminal. In Step 203, the terminal encrypts the random number with the user's unique key and a predetermined algorithm. Then in Step 204, the encrypted result is transmitted back to the cellular-service provider. There, the same random number is encrypted, again with the user's unique key and the same predetermined algorithm. In Step 206 this encrypted result independently calculated by the cellular service provider is compared with that transmitted from the cellular terminal. If the comparison is a match, the caller is "authenticated" and the call is allowed to proceed. Otherwise, authentication fails, and the user is refused access to the cellular network.

Unfortunately, the above described authentication procedure is not entirely satisfactory. It involves extensive calculation at both the user's terminal and the cellular service provider, as well as a number of transmissions between the two. Since a call is not allowed to proceed until the entire authentication is completed, call processing may be significantly delayed.

In addition, it is relatively simple to scan or monitor cellular phone transactions such as the above-

described authentication procedure. Therefore, an unauthorized individual can easily obtain the random number and encrypted response transmitted between the terminal and the cellular service provider. In addition, the predetermined algorithm used in encryption will often be well known in the art, e.g., CAVE algorithm. Thus, the only unknown for the unauthorized individual intending to circumvent the authentication security procedure via scanning is the user's unique key, which unfortunately may be decoded once the random number, encrypted result and ciphering algorithm are known. In fact, unauthorized cellular phone use is not unusual, and has significantly increased the industry's cost of doing business.

Therefore, what is needed is an improved authentication procedure which does not unduly delay call processing and at the same time renders unauthorized cellular use less likely.

SUMMARY OF THE INVENTION

It is an object of the present invention to greatly increase the difficulty of stealing and/or decoding of cellular phone encryption keys.

It is another object of the present invention to prevent fraudulent cellular use occurring as a result of interception of transmission of encryption key data.

It is yet another object of the present invention to provide a user-authentication for cellular-phone use, which method distributes transmission and calculation of messages/data utilized in the authentication method over

more than one call.

The present invention achieves the above objects by providing an alternative to the conventional authentication procedure. In accordance with the present invention, when a subscriber signs on for service, the subscriber is provided with a unique key and an initial encrypted number. The initial encrypted number may be stored in the subscriber's terminal. The cellular-service provider's Home Location Register also stores the same unique key and initial encrypted number in a database record associated with the subscriber.

Once these preliminary steps are taken, the following improved authentication procedure according to the present invention may be utilized. When the subscriber's terminal goes off hook, i.e., when the user intends to make or receive calls, the encrypted result stored in the terminal is transmitted to the cellular-service-provider station which compares the result to its own stored encrypted result. If the results match, the call is allowed to proceed. If not, the user is rejected access to the cellular network.

During the call, the cellular-service-provider station transmits a random number to the terminal. The terminal and cellular-service-provider station then independently encrypt the random number with the same ciphering algorithm and user's unique key. The encrypted results are then stored at their respective locations at the terminal and cellular-service-provider station, replacing the encrypted results stored earlier. These encrypted results are in turn used the next time access to the cellular network is desired, i.e., the next time

the phone goes off hook. Each subsequent time the phone goes off hook, the authentication procedure is again initiated from the terminal with transmission of its previously stored encrypted result for comparison at the cellular-service-provider station.

As should be clear from the above description, the improved authentication procedure according to the present invention allows call processing to proceed more quickly. The call is allowed to proceed immediately, after transmission of an encrypted result from the terminal and a successful comparison of the encrypted result at the cellular-service-provider station. Call processing is not delayed by the transmission of the random number, or by any calculation at the cellular provider station or the terminal, as these take place after access to the cellular network is already allowed.

In addition, the authentication procedure according to the present invention is an improvement on current practice in that the random number and the encrypted result obtained from that random number are not transmitted during the same call. Rather, for each call attempt, the previously stored encrypted result (obtained from the random number transmitted during the preceding call) and a new, unrelated random number (used to obtain a new encrypted result for a future call) are transmitted. Without both the encrypted result and the random number used to obtain it, it is substantially harder to determine the user's unique key. Furthermore, it would be impossible to decode the user's unique key by scanning just one call. Persons using a scanner to obtain information transmitted between the terminal and cellular-service-provider station would have to scan two

distinct calls to have any possibility of decoding the user's key. As these calls may be hours or days apart, the possibility of decryption is significantly reduced.

Further objects and advantages of the present invention will become apparent from a review of the detailed description provided below.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates the apparatus of a GSM cellular network, which is one possible implementation of the apparatus which utilizes the method of the present invention.

FIG. 2 is a flow chart depicting an authentication procedure and one possible embodiment of the method of the present invention.

FIG. 3 is a flow chart depicting an authentication procedure in current use and is provided for comparison purposes to illustrate the advantages and benefits the present invention.

DETAILED DESCRIPTION OF THE INVENTION

In one possible implementation, the method according to present invention may be used in a Global System for Mobile Communications ("GSM") type cellular network, the primary functional components of which network are shown in FIG. 1. It should be noted that FIG. 1 is by no means intended to describe in detail a GSM cellular network, but rather is a basic overview of certain major functional components sufficient to illustrate the method

according to the present invention described herein.

Turning now to FIG. 1, the cellular terminal 1, also referred to as "mobile equipment," is portable, and held by a subscriber. For purposes of the present description, the cellular terminal 1 is assumed to be a cellular phone, but the present invention is of equal benefit to an individual attempting a fax or other transmission. The subscriber also carries a Subscriber Identity Module ("SIM") 6. Stored within the SIM 6 is an authentication key unique to the subscriber. When making a call, the subscriber inserts the SIM 6 into a slot on the cellular terminal 1, so that the cellular terminal 1 may read and transmit the authentication key each time the subscriber wishes to log on to the cellular network.

Cellular transmissions from the cellular terminal 1 are received at a Base Transceiver Station ("BTS") 2, which includes a series of radio transmitters. Each BTS 2 covers a certain range in a discrete area. Accordingly, during a call the subscriber carrying a cellular terminal 1 may move in out of the range of a given BTS 2.

Continuing with FIG. 1, a Base Station Controller ("BSC") 3, which ensures call maintenance, is connected to a group of BTS's 2. Specifically, during a call, the cellular terminal 1 continuously transmits to the BSC 3 the signal strength of each of the group of associated BTS's 2. The BSC 3 can then use these transmissions to determine whether the call should be switched to a new BTS 2, i.e., whether the cellular terminal 1 transmissions should be sent to a new BTS 2.

From the BTS's 2, the cellular terminal 1 transmissions are received at the Mobile Switching Center ("MSC") 4, which routes all incoming and outgoing transmissions to and from fixed-line telephone networks 5 (such as Public Switched Telephone Networks ("PSTN") or Integrated Services Digital Network ("ISDN")) or other cellular networks. From such telephone networks, the call connection is completed.

The MSC 4 shown in FIG. 1 is the heart of the cellular-service-provider's network. The MSC's 4 functions include maintaining all necessary administrative and other subscriber information, such as registration and authentication information and location updates. Thus, the MSC 4 includes a number of databases, including the Home Location Register ("HLR") 7 and associated Authentication Center ("AuC") 9. When access to the cellular network is desired, the HLR 7 generally provides the functionality and information necessary for properly allowing or disallowing access. The AuC 9 also plays a role in this process by providing functionality and information necessary for the HLR 7 to authenticate a particular call. For example, when the HLR 7 receives a log-on request transmitted from the cellular terminal 1, the HLR 7 checks a signed response ("SRES"), which is a portion of the log-on request transmission from the terminal, against an encrypted result generated by the AuC 9 for the subscriber. If the SRES transmitted from the cellular terminal 1 is the same as the encrypted result generated by the AuC 9, the MSC 4 transmits to the cellular terminal 1 a message allowing network access. Otherwise, access to the cellular-phone-network is disallowed.

The steps and operation of the authentication procedure according to the present invention, including the respective role of the HLR 7, AuC 9 and SRES, and advantages resulting from practice of the present invention, will become apparent from the following detailed description.

Turning now to FIG. 2, a flow chart depicting an authentication procedure which is one possible embodiment of the method of the present invention, the authentication procedure according to the present invention assumes that certain preliminary administrative matters have been completed.

Specifically, when a subscriber signs on for service with the cellular-service-provider, the subscriber receives a cellular terminal 1 as well as an SIM 6 card. As is common practice, an authentication key unique to the subscriber is stored in the SIM 6. In addition, a unique "initial encrypted result," i.e., the above mentioned SRES is also stored in the cellular terminal 1. Both the subscriber's unique key and initial encrypted result are also stored in the AuC 9 of the MSC 4 as part of a database record associated with the subscriber. The subscriber is instructed to carry the SIM 6 with the cellular terminal 1, and to insert the SIM 6 into the cellular terminal 1 whenever the subscriber wishes to make or receive calls.

Once the subscriber signs on for service, the following authentication procedure, illustrated in FIG. 2, may be practiced whenever the subscriber wishes to make or receive calls. In Step 100, the subscriber at a cellular terminal 1 indicates an intent to make a call by

taking the phone "off hook," e.g., by pressing a button or flipping a microphone, and inserting the SIM 6 into the cellular terminal 1. As a result, in Step 101, the cellular terminal 1 transmits the "SRES" stored within it to the appropriate BTS 2, and ultimately to the HLR 7. In general, the SRES is the encrypted result (stored in the cellular terminal 1) derived from a random number ("RAND," transmitted from the AuC 9 during a prior call) by manipulation using the subscriber's unique key (stored in the SIM 6) and a ciphering algorithm, such as CAVE. However, as noted above, in the case of the subscriber's first call, the SRES is the initial encrypted result which the cellular service provider causes to be stored in the cellular terminal 1 prior to distribution.

When the SRES is received at the HLR 7, in Step 102, the HLR 7 checks the SRES against an encrypted result stored in a database record associated with the subscriber in the AuC 9. Again, if the subscriber's attempted call is the first request for network access, the encrypted result stored in the AuC 9 for the subscriber will be the same as the SRES stored by the cellular provider in the cellular terminal 1 prior to distribution of the terminal 1 to the subscriber. Otherwise, the encrypted result stored in the AuC 9 is derived from a random number (RAND, transmitted during a prior call to the cellular terminal 1) by manipulation using the subscriber's unique key (also stored in the AuC 9) and the same ciphering algorithm used at the cellular terminal 1, such as CAVE.

If the encrypted result stored in the AuC 9 does not match the SRES transmitted from the cellular terminal 1,

then in Step 103 the HLR 7 rejects the request for cellular network access. Otherwise, if the encrypted result stored in the AuC 9 matches the SRES transmitted from the cellular terminal 1, then in Step 104 the call is allowed and a message to that effect is transmitted back to the cellular terminal 1.

Assuming the call is allowed to proceed, the authentication procedure according to the present invention continues and the call is connected. During call processing, in step 105, the AuC 9 generates a new random number (RAND). Then, in step 106, the AuC 9 uses the same ciphering algorithm as the one used by the cellular terminal 1 to independently derive an encrypted result based on (RAND) and the subscriber's unique key stored in the AuC 9. In Step 107, the latest encrypted result of the ciphering algorithm is stored in the subscriber's database record in the AuC 9 for use in connection with a future request for network access, and the existing encrypted result previously stored in the AuC 9 is deleted.

Once finished with its own encryption processing the AuC 9 transmits the (RAND) generated in Step 106 to the cellular terminal 1 in Step 108. In Step 109, like the AuC 9, the cellular terminal 1 then performs the same ciphering algorithm on the (RAND) using the subscriber's unique key stored in the SIM 6. The encrypted result, i.e., the SRES obtained from applying the ciphering algorithm in Step 109 is stored in the terminal in Step 110 for a future network access request, thus replacing the previously stored SRES in the terminal.

Once the call has been completed, and the subscriber makes another network-access request, the above-described authentication process will be repeated, beginning with step 100.

A few points regarding the above embodiment of the present invention are worthy of note. First, call processing continues after transmission of an encrypted result from the cellular terminal 1 and a successful comparison or verification of the encrypted result at the AuC 9. Call processing is not delayed by the transmission of (RAND) or by the processing of a ciphering algorithm at the AuC 9 or the cellular terminal 1.

In addition, the (RAND) and the encrypted result derived from the (RAND) are not transmitted during the same call. Rather, for each call attempt, the previously stored encrypted result, which is derived from the random number transmitted during an earlier call, and a new, unrelated random number, which is used to derive the encrypted result for a future call authentication, are transmitted. Thus, it would be substantially impossible to decode the subscriber's unique key scanning just one call.

Finally, it should be noted that while the present invention has been described in the above specification, in connection with an exemplary embodiment, the present invention is by no means limited thereby. Numerous minor modifications and alterations may be made to the above described embodiment without departing from the scope of the present invention. For example, although the ciphering algorithms used by the cellular terminal 1 and the AuC 9 have been described as being identical, it need

not be so: the cellular terminal, and the AuC 9 may use different ciphering algorithms as long as both algorithms produce an identical encrypted result based on the same input. In addition, although the ciphering algorithm used in the present invention has been described as the CAVE algorithm, any other number-manipulating algorithm may be used as the ciphering algorithm.

What Is Claimed Is:

1. As a part of a cellular-phone-call-initiating process, a method for authenticating a caller seeking access to a telephone network via transmission from a cellular terminal through a cellular-phone-service-provider station, each of said cellular terminal and said cellular-phone-service-provider station having a previously stored encrypted result and a unique key assigned to the caller, the method comprising the steps of:

a. transmitting, from said cellular terminal, said previously-stored encrypted result to said cellular-phone-service-provider station;

b. authenticating by comparison whether said encrypted result transmitted from said cellular terminal matches said encrypted result previously stored in said cellular-phone-service-provider station;

c. calculating, at the cellular-phone-service-provider station, a new encrypted result by means of a first ciphering algorithm using a random number and said unique key assigned to the caller;

d. transmitting said random number from said cellular-phone-service-provider station to said cellular terminal; and

e. independent of said calculation in step (c), calculating, at the cellular terminal, said new encrypted result by means of a second ciphering algorithm using said transmitted random number and said unique key assigned to the caller;

wherein said new encrypted result calculated in step (c) is stored in said cellular-phone-service-provider

station and said new encrypted result calculated in step (e) is stored in said cellular terminal for next authentication attempt.

2. The method according to claim 1, further comprising the step of:

between steps (b) and (c), facilitating access to the telephone network for the caller if said encrypted result transmitted from said cellular terminal matches said encrypted result previously stored in said cellular-phone-service-provider station.

3. The method according to claim 2, wherein said step of facilitating access to the telephone network is performed at said cellular-phone-service-provider station.

4. The method according to claim 3, wherein step (b) is performed at said cellular-phone-service-provider station.

5. The method according to claim 4, wherein said first ciphering algorithm is a CAVE algorithm.

6. The method according to claim 5, wherein said second ciphering algorithm is a CAVE algorithm.

7. The method according to claim 6, wherein said cellular terminal comprises a cellular telephone and said cellular-phone-service-provider station comprises a mobile switching center.

8. The method according to claim 1, wherein step (b) is performed at said cellular-phone-service-

provider station.

9. The method according to claim 8, further comprising the step of:

between steps (b) and (c), facilitating access to the telephone network for the caller if said encrypted result transmitted from said cellular terminal matches said encrypted result previously stored in said cellular-phone-service-provider station.

10. The method according to claim 9, wherein said first and second ciphering algorithms are a CAVE algorithm.

11. A method for authenticating a caller seeking access to a telephone network via transmission from a cellular terminal through a cellular-phone-service-provider station, which method minimizes the amount of transmission and calculation involved in authenticating said caller, each of said cellular terminal and said cellular-phone-service-provider station having a previously stored check message and a unique key assigned to the caller, the method comprising the steps of:

a. transmitting, from said cellular terminal, said previously-stored check message to said cellular-phone-service-provider station;

b. authenticating by comparison whether said check message transmitted from said cellular terminal matches said check message previously stored in said cellular-phone-service-provider station;

c. facilitating access to the telephone network for the caller if said check message transmitted from said cellular terminal matches

said check message previously stored in said cellular-phone-service-provider station;

d. calculating, at the cellular-phone-service-provider station, a new check message by means of a first ciphering algorithm using a first check element and a second check element;

e. transmitting said first check element from said cellular-phone-service-provider station to said cellular terminal; and

f. independent of said calculation in step (d), calculating, at the cellular terminal, said new check message by means of a second ciphering algorithm using said transmitted first check element and said second check element;

wherein said new check message calculated in step (d) is stored in said cellular-phone-service-provider station and said new check message calculated in step (f) is stored in said cellular terminal for next authentication attempt.

12. The method according to claim 11, wherein said first check element comprises a random number.

13. The method according to claim 12, wherein said second check element comprises said unique key assigned to the caller.

14. The method according to claim 13, wherein said first ciphering algorithm is a CAVE algorithm.

15. The method according to claim 14, wherein said second ciphering algorithm is a CAVE algorithm.

16. The method according to claim 15, wherein

said cellular terminal comprises a cellular telephone and said cellular-phone-service-provider station comprises a mobile switching center.

17. The method according to claim 16, wherein said method is automatically initiated each time said cellular terminal is activated for use.

18. The method according to claim 17, wherein said telephone network comprises one of a PSTN-type network and an ISDN-type network.

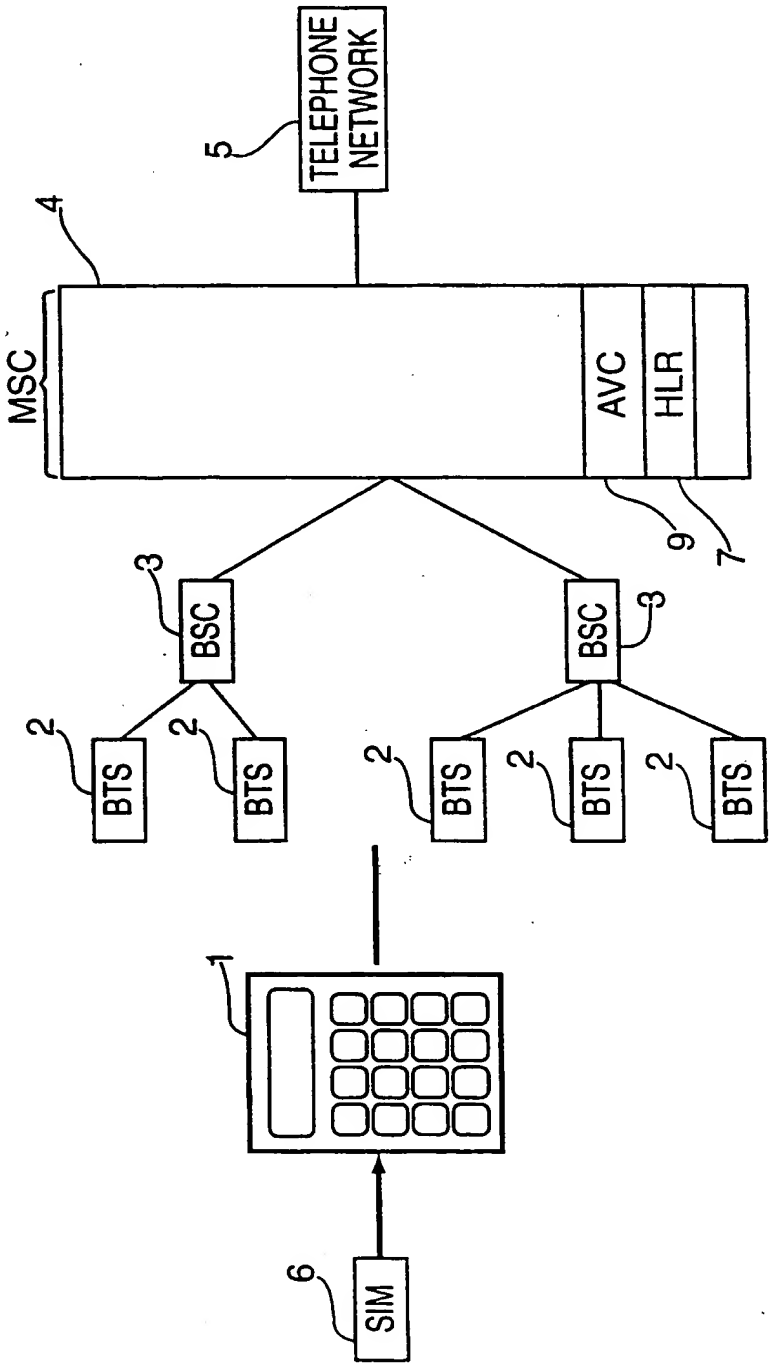

TELEPHONE NETWORK
5
4
MSC
AVC
HLR
9
7
3
BSC
BSC
3
2
BTS
BTS
BTS
BTS
BTS
2
1
6
SIM

FIG. 1

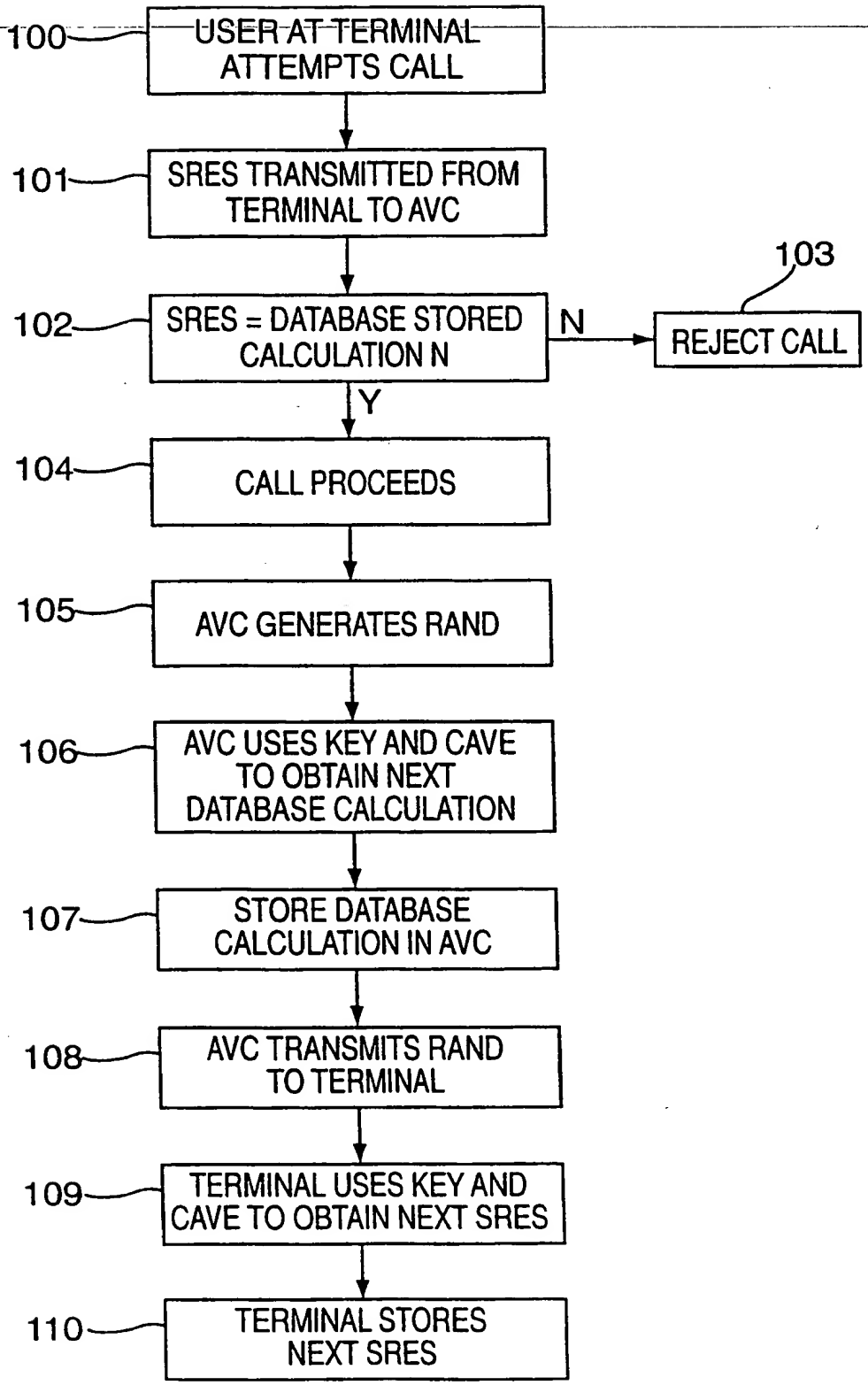

100
USER AT TERMINAL ATTEMPTS CALL
101
SRES TRANSMITTED FROM TERMINAL TO AVC
102
SRES = DATABASE STORED CALCULATION N
N
103
REJECT CALL
Y
104
CALL PROCEEDS
105
AVC GENERATES RAND
106
AVC USES KEY AND CAVE TO OBTAIN NEXT DATABASE CALCULATION
107
STORE DATABASE CALCULATION IN AVC
108
AVC TRANSMITS RAND TO TERMINAL
109
TERMINAL USES KEY AND CAVE TO OBTAIN NEXT SRES
110
TERMINAL STORES NEXT SRES

FIG. 2

This Page Blank (uspto)

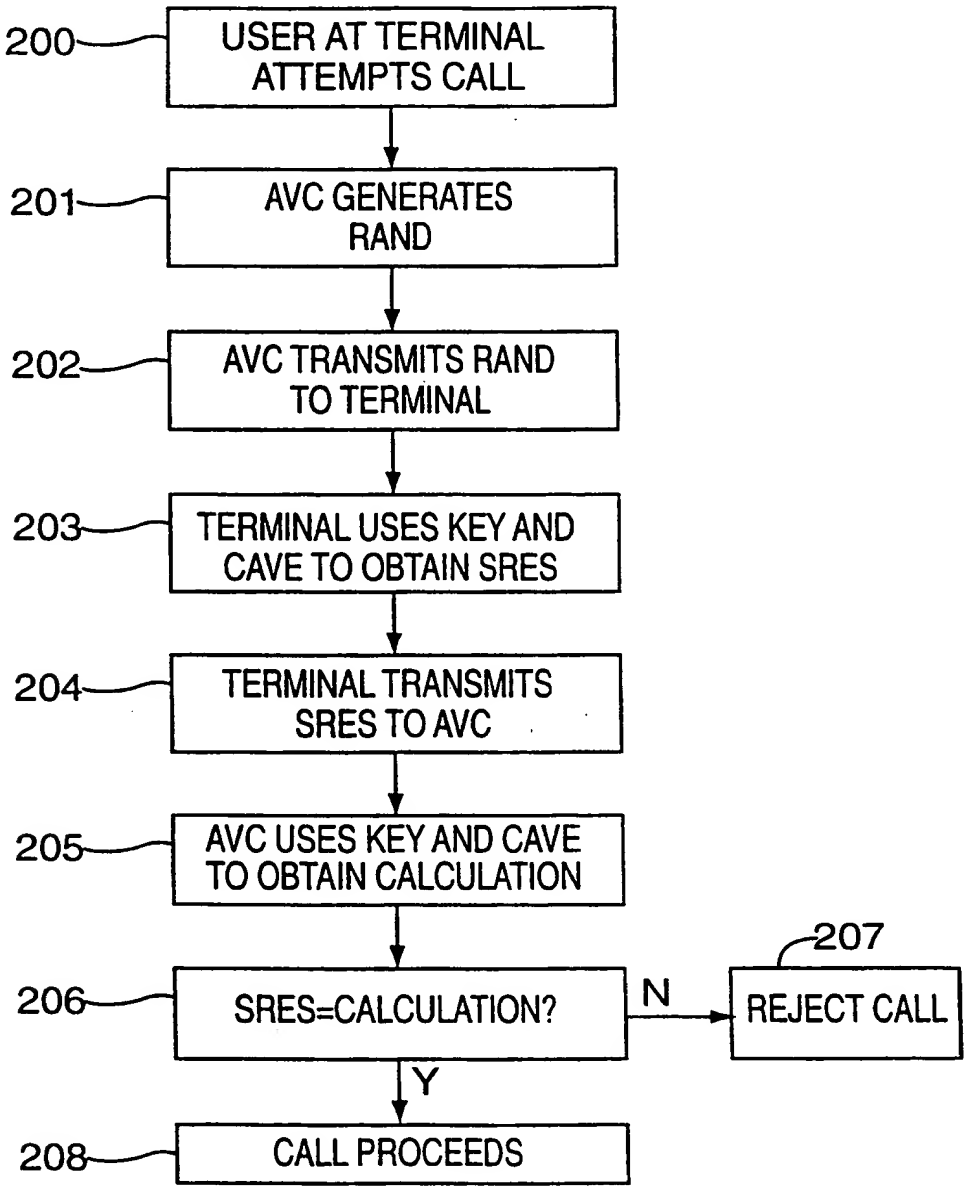


FIG. 3
PRIOR ART

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/06426

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04L 9/32; H04Q 7/22
US CL :380/23; 455/411

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/49; 455/410

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS, search terms: cellular(2a)authentication, CAVE(2a)algorithm, random number

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,390,252 A (SUZUKI ET AL) 14 FEBRUARY 1995, column 11, line 4 through column 13, line 33; Figure 9.	1-18
A	US 5,237,612 A (RAITH) 17 AUGUST 1993, column 6, lines 18-37.	1-18
A	US 5,282,250 A (DENT ET AL) 25 JANUARY 1994, column 2, line 51 through column 3, line 22.	1-18

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 26 MAY 1999	Date of mailing of the international search report 16 JUN 1999
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer GILBERTO BARRÓN JR. Joni Hill Telephone No. (703) 305-1830

Form PCT/ISA/210 (second sheet)(July 1992)*